<u>REMARKS</u>

The present application has been reviewed in light of the Office Action dated December 23, 2008. Claims 4, 5, and 17-20 are presented for examination, of which Claims 4, 17, and 19 are in independent form. Claims 1, 2, and 6-9 have been canceled, without prejudice or disclaimer of the subject matter presented therein, and new Claims 17-20 have been added to provide Applicants with a more complete scope of protection. Claims 4 and 5 have been amended to define aspects of Applicants' invention more clearly. Support for the claim amendments may be found, for example, in FIGS. 14 and 15 and the descriptions thereof in the specification. Favorable consideration is requested.

The Office Action states that Claims 1, 2, 5, 8, and 9 are objected to because of informalities. Cancellation of Claims 1, 2, 8, and 9 renders the objections thereto moot. Line 3 of Claim 5 has been amended to recite "the encrypted encoded image data" to clarify that the "encrypted encoded image data" recited in line 2 of Claim 5 is being referred to in line 3. It is believed that the objections to the claims have been obviated, and their withdrawal is therefore respectfully requested.

The Office Action states that Claims 1, 2, and 5-9 are rejected under 35 § 103(a) as being unpatentable over U.S. Patent No. 6,047,069 (*Hogan*) in view of U.S. Patent Application Publication No. 2003/0237040 (*Lin*) and U.S. Patent Application Publication No. 2003/0066018 (*Yu et al.*); and that Claim 4 is rejected under § 103(a) as being unpatentable over *Hogan* in view of *Lin* and *Yu et al.* and further in view of U.S. Patent Application Publication No. 2003/0091054 (*Futenma*). Cancellation of Claims 1, 2, and 6-9 renders their rejections moot. For at least the following reasons, Applicants submit that independent Claims 5, 17, and 19, together with the claims dependent therefrom, are patentably distinct from the cited prior art.

The aspect of the present invention set forth in Claim 5 is directed to an information processing method for decrypting encrypted encoded image data. The encrypted encoded image data and corresponding header data are received. The header data includes a first field and a second field. The first field stores information indicating whether the encoded image data has an error detecting code for detecting an error in the encoded image data and is referenced by a decoding process. The second field stores information indicating whether the encoded image data has the error detecting code for detecting the error in the encoded image data and is not referenced by the decoding process.

A determination is made, based on the information stored in the second field, regarding whether the encrypted encoded image data includes an error-detecting code. In addition, a determination is made regarding whether key information required to decrypt the encrypted encoded image data is available.

Notably, if the information stored in the second field indicates that the encrypted encoded image data includes the error detecting code and the key information is available, the encrypted encoded image data is decrypted and the first field is modified to store information indicating that the encrypted encoded image data includes the error detecting code. If the information stored in the second field does not indicate that the encrypted encoding image data includes the error detecting code and the key information is available, the encrypted encoded image data is decrypted and the first field is not modified. If the key information is not available, the encrypted encoded image data is not decrypted and the first field is not modified (regardless of the information stored in the second field).

By virtue of the notable features of Claim 5, an apparatus can take advantage of error correction codes included with, for example, JPEG 2000 encoded data that has been

encrypted and, thus, generate fewer decoding errors.[1] Accordingly, when the apparatus receives the data via a network, the apparatus requests fewer retransmissions of image data that cannot be decoded due to errors in the data that occurred during an original transmission of the data. The apparatus realizes these advantages using information stored in the second field of the header data, which is not used by the decoder. More particularly, if the information stored in the second field indicates that the data includes the error detecting code and the key information is available, the data is decrypted and the first field is modified to store information indicating that the encrypted encoded image data includes the error detecting code, which is used by the decoder to correct errors in the data.

Hogan relates to encryption of original data and associated redundancy bytes while retaining error correction capabilities of the original data. (*see* Abstract). *Hogan* discusses that a drive can transfer a seed number NR to an MPEG decoder, which the decoder uses to generate a pseudo-random data sequence that is used for decryption (*see* col. 6, lines 7-15). As best understood by Applicants, *Hogan* is silent regarding using first and second header fields, where the second header field is not used by a decoding process, and where the first header field is modified if the second header field indicates that encrypted encoded image data includes an error-detecting code. Moreover, *Hogan* is silent regarding the conditional "decrypting" recited in Claim 5.

Lin relates to a method of playing an MP3 file and providing error checking protection when error checking fields exist in an MP3 bitstream, and playing the MP3 bitstream without error checking when the error checking fields do not exist in the MP3 bitstream (*see*

[1/] Any examples presented herein are intended for illustrative purposes and are not to be construed to limit the scope of the claims.

paragraph 2). *Lin* discusses that a frame has a header including a protection bit, which indicates whether error protection is used in the frame (*see* paragraph 5, lines 6-10). As best understood by Applicants, *Lin* is silent regarding using first and second header fields, where the second header field is not used by a decoding process, and where the first header field is modified if the second header field indicates that encrypted encoded image data includes an error-detecting code. Moreover, *Lin* is silent regarding the conditional "decrypting" recited in Claim 5.

Yu et al. relates to a method of stopping iterative decoding caused by an occurrence of an error (*see* paragraph 3). *Yu et al.* discusses that a turbo decoder 610 performs error correction and decoding on frames of data (*see* paragraph 90, lines 1-3). A Cyclic Redundancy Check (CRC) checker 612 may detect an error in each frame using CRC bits for decoded output from the turbo decoder 610 (*see* paragraph 90, lines 3-7). The CRC checker 612 outputs a result signal CRC_FLAG for a CRC check, wherein, if the CRC check result is "good," the CRC checker 612 may switch the CRC_FLAG from "0" to "1" to stop the decoding (*see* paragraph 90, lines 7-10).

Yu et al. also discusses that a Log Likelihood Ratio (LLR) stop controller 614 tests a LLR-based decoding stop condition (*see* paragraph 90, lines 10-12). If a frame satisfies the LLR-based decoding stop condition, the LLR stop controller 614 switches a LLR_FLAG signal from "0" to "1" to stop the decoding (*see* paragraph 90, lines 16-19). A stop selection controller 616 receives the CRC_FLAG signal from the CRC checker 612 and the LLR_FLAG signal from the LLR stop controller 614 and selects a decoding stop mode based on the two inputs (*see* paragraph 90, lines 19-23). If the CRC_FLAG signal or the LLR_FLAG signal of the selected decoding stop mode is "1," the stop selection controller 616 outputs a control signal STOP_TURBO for stopping the decoding being performed by the turbo decoder 610, wherein

the stop selection controller 616 may switch the STOP_TURBO signal from "0" to "1" to stop further decoding (*see* paragraph 90, lines 23-31). The decoding stop modes are selected based on a control signal MODE_SELECT (*see* paragraph 90, lines 31-33).

Further, *Yu et al.* discusses that, in a case where only a CRC-based decoding stop mode is used, if the CRC_FLAG signal is changed from "0" to "1," the STOP_TURBO signal also is changed from "0" to "1," thus stopping the decoding (*see* paragraph 90, lines 33-36). As best understood by Applicants, various control signals are set based on error conditions encountered while decoding a frame of data. Nothing has been found in *Yu et al.* that is believed to teach or suggest using first and second header fields, where the second header field is not used by a decoding process, and where the first header field is modified if the second header field indicates that encrypted encoded image data includes an error-detecting code. Moreover, *Yu et al.* is silent regarding the conditional "decrypting" recited in Claim 5.

Applicants submit that a combination of *Hogan*, *Lin*, and *Yu et al.*, assuming such combination would even be permissible, would fail to teach or suggest an information processing method that includes "modifying the first field to store information indicating that the encrypted encoded image data includes the error detecting code, if the information stored in the second field indicates that the encrypted encoded image data includes the error detecting code and the key information is available, wherein the first field is not modified, if the information stored in the second field does not indicate that the encrypted encoding image data includes the error detecting code and the key information is available, and wherein, if the key information is not available, the first field is not modified" "decrypting the encrypted encoded image data to generate encoded image data, if the information stored in the second field indicates that the encrypted encoded image data includes the error detecting code and the key information is

available" and "decrypting the encrypted encoded image data, if the information stored in the second field does not indicate that the encrypted encoding image data includes the error detecting code and the key information is available, wherein, if the key information is not available, the encrypted encoded image data is not decrypted" as recited in Claim 5. Accordingly, Applicants submit that Claim 5 is patentable over *Hogan*, *Lin*, and *Yu et al.*, and respectfully request withdrawal of the rejection under 35 U.S.C. § 103(a).

Independent Claims 17 and 19 include features similar to those of Claim 5 and are believed to be patentable for at least the reasons discussed above. The other claims in the present application depend from one or another of independent Claims 1, 17, and 19 and are submitted to be patentable over *Hogan*, *Lin*, and *Yu et al.* for at least the same reasons. Because each dependent claim also is deemed to define an additional aspect of the invention, individual consideration of the patentability of each claim on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and an early passage to issue of the present application.

No petition to extend the time for responding to the Office Action is deemed necessary for this Amendment. If, however, such a petition is required to make this Amendment timely filed, then this paper should be considered such a petition and the Commissioner is authorized to charge the requisite petition fee to Deposit Account 06-1205.

Applicants' undersigned attorney may be reached in our New York Office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address listed below.

Respectfully submitted,

/Jonathan Berschadsky/
Jonathan Berschadsky
Attorney for Applicants
Registration No. 46,551

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

FCHS_WS 2751327v3